8 HARD DRIVE IMAGING

8.1 Purpose

To provide the proper procedures for the imaging of a hard drive or other digital media.

8.2 Scope

This document contains the procedures for the proper collection and preservation of digital forensic evidence. Making an image of a computer's or DVR's hard drive is not the same as making a copy of the hard drive. When a hard drive is copied, only the logical files are written onto the target drive. When an image is created from a hard drive, all of the information on the hard drive is written to the target drive, including the slack space, unallocated space and deleted files.

8.3 Materials - Equipment (Hardware/Software)

The following equipment and materials may be utilized:

- Computer hardware and software
- Talon
- Video players and recorders (analog and digital)
- Conventional and digital cameras
- Cell phones
- Digital media (floppy disk, CD's, DVD's, flash cards, thumb drives, and hard drives)
- Other image storage devices
- Standard computer tools
- Forensic imaging hardware and software

8.4 Limitations

None for this procedure

8.5 Safety

None for this procedure

8.6 Procedures

8.6.1 Insert the evidence hard drive and target drive into the computer.

8.6.2 Boot the computer in DOS using an approved forensic boot disk or Linux boot disk/CD.

- CAUTION: While the evidence hard drive is in the computer, the computer must not be booted in a Windows mode. Booting in Windows can change files on the evidence hard drive.

8.6.3 Make a mirror image copy of the evidence hard drive onto the target drive using the Safe back, Linux dd or Smart program located on the boot disk.

8.6.4 Use write blocking hardware device or write blocking software to ensure that the evidence computer's drive is locked and unlock the target drive.

- CAUTION: Locking the evidence computer's hard drive ensures that the target drive cannot be accidentally copied onto the evidence computer's hard drive. Ensure that the evidence computer's hard drive is locked.

8.6.5 Execute an MD-5 or other accepted hash algorithm of the evidence hard drive.

8.6.6 Image the evidence hard drive using the approved software.

8.6.7 Execute an MD-5 or other accepted hash algorithm of the image that was created.

8.6.8 Execute an MD-5 of other accepted hash algorithm of the evidence hard drive to verify that nothing has been altered.

8.6.9 Examine the target drive with an approved anti-virus program to ensure that it has not been infected by the evidence computer's hard drive.

8.6.10 After verifying that the copy has been successfully completed, remove the evidence computer's hard drive from the computer.

8.6.11 Documentation of the process will be in the case file notes and may be in the form of printouts.

8.7 References

Owner's Manuals, User's Manuals and appropriate software manuals should be referenced for equipment and operating instructions.

Best Practices for the retrieval of video evidence for digital CCTV systems.

Logicube desktop User's Manual

Digital Intelligence User's Manual

Bigelow, Stephen J., Troubleshooting, Maintaining and Repairing PCs. 2nd ed. New York, McGraw-Hill, 1999.

Gookin, Dan. DOS for Dummies. 3rd ed. Hoboken, NJ: Wiley Publishing, Inc., 1999.

Groth, David. A+ Complete Study Guide. 3rd ed. San Francisco: SYBEX Inc., 2003.

Kruse, Warren G., and Jay G. Heiser. Computer Forensics Incident Response Essentials. Boston: Addison-Wesley, 2002.

Nelson, Stephen L. Windows XP an Introduction. New York: Barnes and Noble Books, 2002.

Rathbone, Andy. Windows 95 for Dummies. 2nd ed. Foster City, CA: IDG Books Worldwide, 1997.

Electronic Crime Scene Investigation a Guide for First Responders. Washington, D.C.: U.S. Department of Justice, 2001.

Best Practices for Seizing Electronic Evidence a Pocket Guide for First Responders. 3rd ed. Washington, D.C.: U.S. Department of Homeland Security, United States Secret Service.

♦End